Direct dialling of Haar random unitary matrices

2017 New J. Phys. 19 033007

(http://iopscience.iop.org/1367-2630/19/3/033007)

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

RECEIVED
14 November 2016

REVISED
6 February 2017

ACCEPTED FOR PUBLICATION
16 February 2017

PUBLISHED
2 March 2017

PAPER

Direct dialling of Haar random unitary matrices

Nicholas J Russell[1], **Levon Chakhmakhchyan**[2,3], **Jeremy L O'Brien**[1] **and Anthony Laing**[1,3]

[1] Centre for Quantum Photonics, H. H. Wills Physics Laboratory & Department of Electrical and Electronic Engineering, University of Bristol, BS8 1UB, United Kingdom
[2] Centre for Quantum Information and Communication, Ecole polytechnique de Bruxelles, CP 165, Université libre de Bruxelles, B-1050 Brussels, Belgium
[3] Authors to whom any correspondence should be addressed.

E-mail: levon.chakhmakhchyan@ulb.ac.be **and** anthony.laing@bristol.ac.uk

Keywords: optical circuits, integrated optics, Haar random unitary matrices, boson sampling

Abstract

Random unitary matrices find a number of applications in quantum information science, and are central to the recently defined boson sampling algorithm for photons in linear optics. We describe an operationally simple method to directly implement Haar random unitary matrices in optical circuits, with no requirement for prior or explicit matrix calculations. Our physically motivated and compact representation directly maps independent probability density functions for parameters in Haar random unitary matrices, to optical circuit components. We go on to extend the results to the case of random unitaries for qubits.

The development of the boson sampling problem [1–5] has motivated fresh interest in studying Haar random unitary matrices (HRUs) [6] realised with optical circuits to act on multiphoton states. Simultaneously, developments in integrated optics [7–15] now facilitate the construction of large-scale optical circuits capable of actively realising any unitary operator [16] including HRUs. Furthermore, HRUs play an important role in various tasks for quantum cryptography [17] and quantum information protocols [18, 19], as well as the construction of algorithms [20].

Here we present a simple procedure for choosing a HRU on an optical circuit, implemented in terms of recursive decompositions of a unitary operator [21, 22], by choosing values of the physical parameters independently from simple distributions. This procedure is useful for applications where the exact unitary description of the implemented circuit is less important than a guarantee that it is drawn from the correct distribution. While similar parameterisations exist in the mathematical literature [23], an operational application within linear optics is not widely appreciated. We extend the result to systems of qubits, by deriving a mapping between a linear-optical circuit on $m = 2^n$ modes and a circuit operating on n qubits. Note that constructions for pseudo-HRUs on qudit and qubit systems are also available, serving as a general framework to investigate randomising operations in complex quantum many-body systems [24, 25].

Choosing a HRU is analogous to choosing a random number from a uniform distribution, in that it should be unbiased. The probability of selecting a particular unitary matrix from some region in the space of all unitary matrices should be in direct proportion to the volume of the region as defined by the Haar measure, which is the unique translation-invariant measure on the space of unitary matrices. As argued in [26], the columns of an m-dimensional HRU may be made up from vectors $\{v_i\} = \{v_1, v_2, \ldots, v_m\}$ that are successively drawn from the unbiased distribution of unit vectors in the subspace of $(m - i + 1)$ dimensions, orthogonal to all previous vectors. The problem of choosing HRUs thus reduces to the problem of recursively choosing such a set of orthogonal vectors.

As we will show, this approach is particularly relevant to recursive circuit decompositions that allow any unitary matrix to be implemented over m optical modes, by choosing appropriate values for beamsplitter reflectivities and phase shifters. We first consider the *triangular scheme* [16] shown in figures 1, 2(a), which is a variant of that proposed by Reck *et al* [21], and which represents an $m \times m$ unitary matrix U as a product of

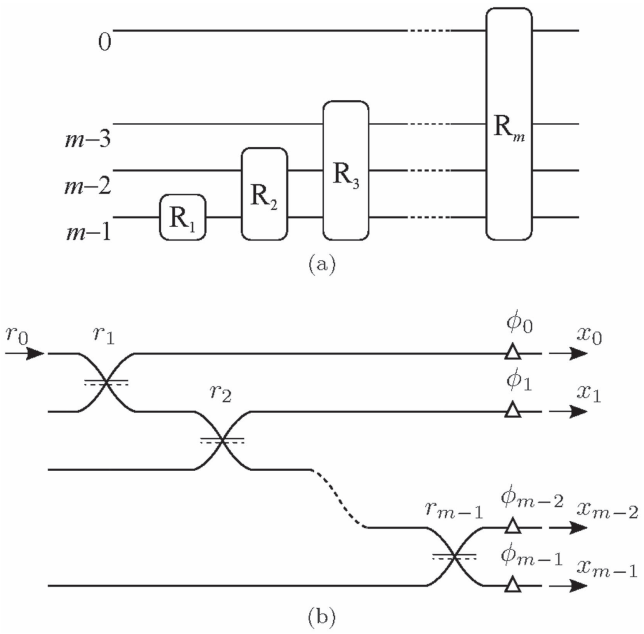

Figure 1. Recursive decomposition of a unitary in the triangular scheme. (a) An $m \times m$ unitary transformation can be factored as a product of m unitary transformations R_i, each acting on a successively larger subspace (the subscripts 0,..., $m-1$ on the left label the modes of the transformation). (b) A linear optical R_m can be constructed from a cascade of beamsplitters and phase shifts on optical modes. Both the *Cartesian* basis, $\mathbf{x}$ and the *physical* basis, $\mathbf{r}$ are illustrated.

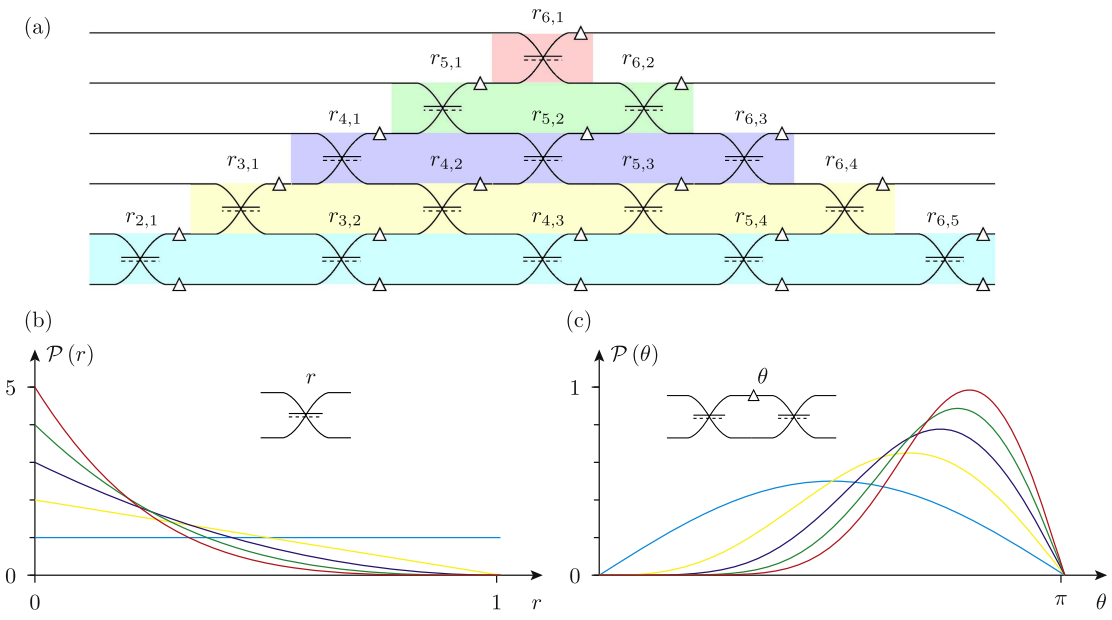

Figure 2. Direct dialling of a HRU in a triangular linear optical circuit. (a) A 6×6 unitary operator implemented with a triangular six mode linear optical circuit. (b) The pdfs from which beamsplitter reflectivities should be chosen to directly implement a HRU. Those on higher rows are chosen according to polynomials with increasing bias towards lower reflectivities. (c) A variable reflectivity beamsplitter can be effectively implemented with an MZI composed of a phase shift, θ between two 1/2 reflectivity beamsplitters. The MZI phases may be chosen directly from the distributions shown, with increasing bias towards $\theta = \pi$. The integrated optics implementation with directional couplers results in a bias towards $\theta = 0$. Line colours in (b) and (c) correspond to shading in (a).

unitary operators labelled R_n, $U = \prod_{i=0}^{m-1} R_{m-i}$ [4]. Each block R_n is chosen to transform the mode $j = m - n$, or the corresponding basis state, denoted by $|\Psi_{m-n}\rangle$, into the n-dimensional unit vector $|v_n\rangle$, over modes $j = m - n$ to $k = m - 1$, i.e.

[4] Note that scheme realised in the integrated photonic chip of [16], in which each beamsplitter in every block R_n couples two adjacent modes, differs from the earlier proposal of [21], in which the first mode is consecutively coupled with modes 2, 3 ,..., n.

$$|v_n\rangle = R_n\ |\Psi_{m-n}\rangle. \tag{1}$$

This vector undergoes further transformations under subsequent blocks R_i $(n < i \leqslant m)$ to finally produce $|f_n\rangle$ that occupies all m modes:

$$|f_n\rangle = R_m \cdots R_{n+1}\ |v_n\rangle. \tag{2}$$

Orthogonality between each of the m $|f_i\rangle$ vectors is guaranteed. Further, if the vector $|v_n\rangle$ is chosen from the unbiased distribution of unit vectors in n-dimensions, the property of left invariance ensures that $|f_n\rangle$ does not become biased by the operation of the subsequent R_i.

The next and main task is therefore determining how an unbiased vector in n-dimensions may be implemented with R_n by choosing values for the linear optical components from which it is constructed, according to the expansion shown in figure 1(b). To achieve this, consider the complex Gaussian vector in n-dimensions:

$$|\mathbf{v}_n\rangle = \sum_{i=0}^{n-1} z_i\ |\Psi_i\rangle = \sum_{i=0}^{n-1} \tau_i e^{i\alpha_i}\ |\Psi_i\rangle, \tag{3}$$

where $|\Psi_i\rangle$ denotes the ith basis state and the z_i are independent and identically distributed normal random variables with the probability density function (pdf), $\mathcal{P}_{z_i}(z) = 1/\pi \exp(-|z|^2)$. This independence means that the pdf for $\mathbf{v}_n$ is the product of the pdfs for these elements and depends only on the magnitude of the vector:

$$\mathcal{P}_{\mathbf{v}_n}(\mathbf{x}) = \frac{1}{\pi^n} e^{-(x_0+x_1+\cdots+x_{n-1})} = \frac{1}{\pi^n} e^{-|\mathbf{v}_n|^2}, \tag{4}$$

where $x_i = |z_i|^2$. We now show how this basis $\mathbf{x}$, which we call the Cartesian basis, can be mapped to a new basis, $\mathbf{r}$. We call the latter the physical basis, since, as we demonstrate below, it contains the variables corresponding directly to components in a physical realisation of the vector in linear optics. Namely, we denote by r_0 the power of the input to the given block R_n, while the other r_i stand for the reflectivities of beamsplitters (see also figure 1(b)). Next, combining the definition (1) and equation (3), we find

$$z_0 = e^{i\phi_0}\sqrt{r_0 r_1}, \tag{5}$$

$$z_i = e^{i\phi_i}\sqrt{r_0 r_{i+1}} \prod_{k=1}^{i} \sqrt{1-r_k} \quad 0 < i \leqslant n-1, \tag{6}$$

where the matrix (in the Pauli basis) $B(r) = \sqrt{r}\,\sigma_z + \sqrt{1-r}\,\sigma_x$ has been used to describe a beamsplitter as a function of its reflectivity. Finally, taking into account that $x_i = |z_i|^2$, we find

$$r_0 = \sum_{k=0}^{n-1} x_k, \tag{7}$$

$$r_i = \frac{x_{i-1}}{\sum_{k=i-1}^{n-1} x_k} \qquad 0 < i \leqslant n-1, \tag{8}$$

$$\phi_i = \alpha_i. \tag{9}$$

We must show that the pdfs for the vector $\mathbf{v}_n$ are separable in the physical basis so that the experimental parameters can be chosen independently. We also need to derive the form of the marginal distributions for the r_i and ϕ_i, from which experimental parameters must be chosen to obtain a Haar unitary. Since there is no functional dependence on the α_i parameters in equation (4) and there is a one-to-one mapping $\alpha_i \to \phi_i$, these phases can be chosen uniformly and independently from the interval $[0,\ 2\pi)$.

Finding the pdfs for the beamsplitter reflectivities requires a more careful change in bases, using the Jacobian

$$\mathcal{P}_{\mathbf{v}_n}(\mathbf{r}) = \mathcal{P}_{\mathbf{v}_n}(\mathbf{x})|\det J(\mathbf{x},\ \mathbf{r})|. \tag{10}$$

The pre-factor from (4) is expressed in the $\mathbf{r}$ basis simply as $\exp(-r_0)$, so is trivially separable. We therefore consider the Jacobian matrix

$$J_{i,j}(\mathbf{x},\ \mathbf{r}) = \frac{\partial x_i}{\partial r_j} \tag{11}$$

with

$$x_0 = r_0\ r_1, \tag{12}$$

$$x_i = r_0\ r_{i+1} \prod_{k=1}^{i} (1-r_k) \qquad 0 < i \leqslant n-1. \tag{13}$$

For the four cases

$$J_{i,j} = r_{i+1} \prod_{k=1}^{i} (1-r_k) \qquad j = 0, \tag{14}$$

$$J_{i,j} = \frac{-r_0 r_{i+1}}{1 - r_j} \prod_{k=1}^{i} (1 - r_k) \qquad 0 < j \leqslant i, \tag{15}$$

$$J_{i,j} = r_0 \prod_{k=1}^{i} (1 - r_k) \qquad j = i + 1, \tag{16}$$

$$J_{i,j} = 0 \qquad j > i + 1, \tag{17}$$

where the variable $r_n = 1$ has been introduced for convenience.

We show that this form of matrix (lower Hessenberg) can always be transformed into a lower triangular matrix—for which the determinant is simply the product of the diagonal elements—by elementary operations, which do not change the absolute value of the determinant.

The first step is to perform a set of operations on the $j = 0$ column, $\mathbf{c}_0$, that set the upper $n - 1$ terms to zero, as follows:

$$\mathbf{c}_0^{(k)} = \mathbf{c}_0^{(k-1)} - \mathbf{c}_k \frac{J_{k-1,0}^{(k-1)}}{J_{k-1,k}}, \tag{18}$$

where k runs from 1 to $m - 1$, $\mathbf{c}_0^{(k)}$ and $J_{k,0}^{(k)}$ are those quantities after k operations, and $\mathbf{c}_k$ is the kth column. We can then place the column $\mathbf{c}_0$ as the rightmost column, at which point the matrix is lower triangular. After the procedure is complete the element $J_{0,n-1} = 1$ (see appendix for detailed proof).

The Jacobian determinant is given by multiplying the diagonal elements of the shifted matrix

$$\mathrm{detJ}(\mathbf{x}, \mathbf{r}) = \prod_{i=1}^{n-1} J'_{i,i} \tag{19}$$

which are given by equation (16). The explicit form of the pdf in the $\mathbf{r}$ basis is

$$\mathcal{P}_{\mathbf{v}_n}(\mathbf{r}) = \mathrm{e}^{-r_0} r_0^{n-1} \prod_{k=1}^{n-1} (1 - r_k)^{n-k-1}, \tag{20}$$

which is manifestly separable.

It can be verified by explicit integration that this expression is appropriately normalised. Since the pdf is separable in this basis, the variables r_i are independent, and can be chosen according to their marginal distributions

$$\mathcal{P}_{r_{n,i}}(r) = (n - i)(1 - r)^{n-i-1} \qquad 1 \leqslant i < n, \tag{21}$$

where, for clarity, $r_{n,i}$ denotes the reflectivity of the ith beamsplitter in the nth rotation, R_n. We now integrate over r_0 to obtain a compact form for the pdf of n-dimensional *unit* vectors

$$\mathcal{P}_{v_n}(\mathbf{r}) = (n - 1)! \prod_{k=1}^{n-1} (1 - r_{n,k})^{n-k-1} \tag{22}$$

and express the pdf for the full circuit of beamsplitters, $\mathcal{P}_{\mathrm{C}}(\mathbf{r})$ as the product of the pdfs for the diagonal arrays of beamsplitters:

$$\mathcal{P}_{\mathrm{C}}(\mathbf{r}) = \prod_{j=1}^{m} \left[(j - 1)! \prod_{k=1}^{j-1} (1 - r_{j,k})^{j-k-1} \right]. \tag{23}$$

Recalling the beamsplitter transformation $B(r) = \sqrt{r}\,\sigma_z + \sqrt{1 - r}\,\sigma_x$, we note that a variable reflectivity beamsplitter can be constructed as a Mach–Zehnder interferometer (MZI), from a variable phase shifter θ between two 1/2 reflectivity beamsplitters, $H = B(1/2)$, to give $B_v(\theta) = \cos\frac{\theta}{2} I + \mathrm{i} \sin\frac{\theta}{2}\sigma_x$ (up to a global phase). It is then useful to re-express the pdfs in terms of MZI phase shifts. The further change of variables, $r = \cos^2\frac{\theta}{2}$, gives

$$\mathcal{P}_{\theta_i}^{\mathrm{B}}(\theta) = (n - i)\cos\frac{\theta}{2}\left[\sin\frac{\theta}{2}\right]^{2(n-i)-1}. \tag{24}$$

In the setting of integrated optics, where beamsplitters are implemented with directional couplers on waveguides according to $D(1/2) = \frac{1}{\sqrt{2}}(I + \mathrm{i}\sigma_x)$ for reflectivity of 1/2, the pdfs are given by (24) but with sin and cos functions interchanged, i.e.

$$\mathcal{P}_{\theta_i}^{\mathrm{D}}(\theta) = (n - i)\sin\frac{\theta}{2}\left[\cos\frac{\theta}{2}\right]^{2(n-i)-1}. \tag{25}$$

In practical terms, an optical circuit composed of beamsplitters and variable phase shifters can directly *dial up* a configuration corresponding to a HRU, by choosing phase shifter values from the derived pdfs. A six mode example is given in figure 2.

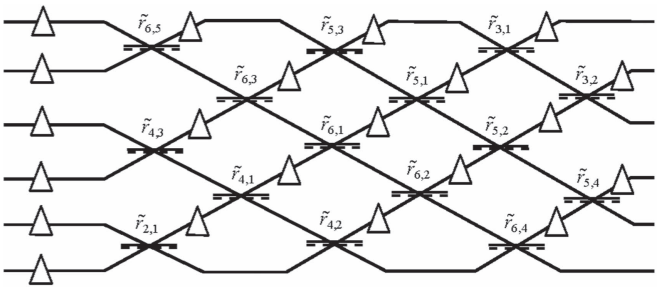

Figure 3. A 6×6 unitary operator implemented with a six-mode linear optical circuit according to the rectangular scheme. Here, $\tilde{r}_{n,i}$ stands for the reflectivity of the ith beamsplitter of the block $\tilde{R}_n$. Within each $\tilde{R}_n$ ($n = 2,..., 6$), we enumerate the beamsplitters according to the sequence s, which consists of $n - 1$ indices, with odd (even) numbers arranged in descending order and followed by even (odd) numbers, arranged in ascending order (see also main text). In this figure, the beamsplitters in the ith row mix the modes $i - 1$ and i (e.g., the beamsplitters of the third row, $\tilde{r}_{4,3}$, $\tilde{r}_{6,1}$ and $\tilde{r}_{5,2}$, couple the modes 2 and 3).

We note that the version of the triangular scheme used here, in which each beamsplitter in every block R_n couples two adjacent modes, differs from the original scheme [21], in which the first mode is consecutively coupled with modes $2, 3,\ldots, n$. It is easy to check, however, that the mapping (7)–(9) can be applied to the original scheme as well, by replacing r with $1 - r$ and relabelling the output modes: $\{x_0, x_1,..., x_{m-1}\} \rightarrow \{x_{m-1}, x_0,..., x_{m-2}\}$. Such a change of variables does not affect the Jacobian determinant and the final expression for the reflectivity pdfs for the original scheme is obtained by replacing r with $1 - r$ in equation (21) (the phases are again chosen uniformly and independently from the interval $[0, 2\pi)$).

Next, we analyse the alternative decomposition of unitary matrices, proposed by Clements *et al* [22], which corresponds to a *rectangular* mesh of beamsplitters and phase shifters, as shown in figure 3 for six modes. While the triangular scheme might be more resilient to loss and other errors in experiments in which only a small proportion of its (upper) input ports are accessed, the rectangular scheme is likely to be beneficial for experiments that involve accessing most of its inputs. The more compact rectangular scheme may also fit a greater number of modes on standard wafers used in the fabrication of integrated photonic circuits.

The rectangular scheme obeys the blocked structure, analogous to the triangular scheme described above. That is, an $m \times m$ unitary matrix U can be written down as a product of blocks $\tilde{R}_n$ (hereafter the tilde refers to the decomposition of [22]). Each of these blocks, as previously, transforms the mode $m - n$ into a vector over modes $m - n$ up to $m - 1$ (see also figure 1(b)). More precisely, for odd (even) m, $U = \prod_{j=1}^{m/2} \tilde{R}_{2j-1} \prod_{i=0}^{m/2-1} \tilde{R}_{m-2i}$ ($U = \prod_{j=1}^{(m-1)/2} \tilde{R}_{2j} \prod_{i=0}^{(m-1)/2} \tilde{R}_{m-2i}$). Moreover, the mapping of equations (7)–(9) for the operator R_n for the triangular scheme can be used for $\tilde{R}_n$ as well, by a simple substitution. Namely, for even (odd) m we replace $\tilde{r}_{n,i}$ by $r_{n,s(i)}$, $\forall\, i$, where s is a sequence of $n - 1$ indices, with odd (even) numbers arranged in descending order and followed by even (odd) numbers, arranged in ascending order (e.g., for $m = n = 6$, we have $s = \{5, 3, 1, 2, 4\}$).

This substitution leaves the corresponding Jacobian determinant unaffected. Therefore, the pdfs given in equation (21) for reflectivities $r_{n,i}$ for the triangular scheme correspond to that of the rectangular scheme, but for $\tilde{r}_{n,s(i)}$. In other words, $\mathcal{P}_{r_{n,i}}(r) = \tilde{\mathcal{P}}_{\tilde{r}_{n,s(i)}}(r)$. Subsequently, we find

$$\tilde{\mathcal{P}}_{\tilde{r}_{n,i}}(\tilde{r}) = [n - s(i)](1 - \tilde{r})^{n-s(i)-1}. \tag{26}$$

Alternatively, one can reorder the reflectivities $\tilde{r}_{n,i}$ according to the sequence s, as is done in figure 3, yielding $\mathcal{P}_{r_{n,i}}(r) = \tilde{\mathcal{P}}_{\tilde{r}_{n,i}}(r)$. Finally, the phases of the rectangular scheme, analogous to the triangular scheme, are chosen uniformly and independently from the interval $[0, 2\pi)$.

Given the above parameterisation of Haar-random optical circuits, we now address the effects of errors, caused by imperfections in integrated photonics manufacturing. Before going into detail, we emphasise the important feature of our approach: due to the separability of the derived probability distributions, errors on a given component of the circuit do not propagate to other independently chosen parameters. In turn, a major source of individual errors is the imperfection of directional couplers. Used to implement the balanced beamsplitters of MZIs, directional couplers should ideally couple $1/2$ of the light between waveguides so that each MZI can achieve the full reflectivity range. Fabrication tolerances, however, introduce errors and limitations on this range. Furthermore, we note that upper MZIs in the triangular scheme and central MZIs in the rectangular scheme are those most sensitive to errors, according to their polynomially growing pdfs.

Although schemes exist to minimise the effect of such errors and produce near perfect MZIs [27, 28] it is worthwhile considering the influence of many small errors over a large circuit (this simple model is also useful to the qubit picture that we develop below). As an estimate to this effect we address the range of unitary operations covered by the proposed parameterisation, which we evaluate in terms of the *coverage* of the unitary space (see

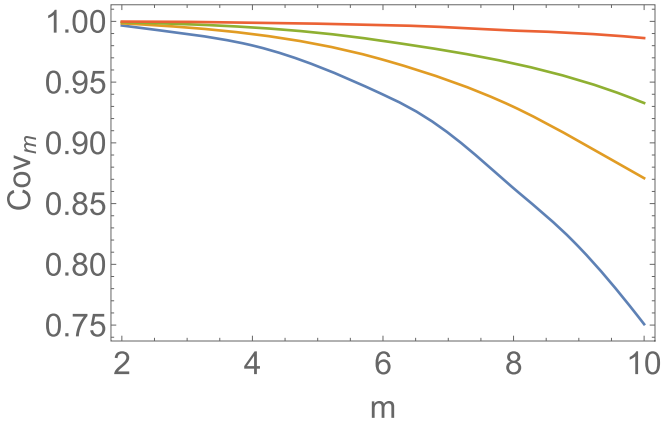

Figure 4. Coverage cov_m of the unitary space versus the circuit size m. The phase shifters are assumed to cover their full range $[0,\ 2\pi)$, while the range of reflectivities is restricted to $[|\varepsilon|,\ 1\ -\ |\varepsilon|]$, where random errors ε are drawn from a zero-mean normal distribution. The curves correspond to different variances σ of the errors ($\sigma = \{1,\ 5,\ 10,\ 20\} \times 10^{-4}$ from the upper to the bottom curve). For each m, the coverage is averaged over many realisations of ε.

[23, 29] for more details)

$$\mathrm{cov}_m = \frac{\prod_{n=2}^{m}\prod_{i=1}^{n-1}\int_{|\varepsilon|}^{1-|\varepsilon|} \mathrm{d}r_{n,i}\,\mathcal{P}_{\nu_n}(\mathbf{r})}{\int_U \mathrm{d}U}. \tag{27}$$

That is, cov_m is the ratio between the reachable and full unitary spaces, assuming that the phase shifters cover their full range $[0,\ 2\pi)$. The range of MZI reflectivities, in turn, is $[|\varepsilon|,\ 1\ -\ |\varepsilon|]$, where ε is a small random error. In figure 4 we plot the coverage versus the circuit size m, which shows that for such moderate errors our parameterisation achieves high coverage rates. Since the pdfs for the triangular and rectangular schemes have been shown to be equivalent and independent, the coverage plotted in figure 4 is valid for both.

We now briefly show how these results may be extended to the scenario of quantum information processing with qubits, independently of any particular physical implementation. We suggest a mapping between a unitary operation on $m = 2^p$ optical modes and the same unitary operation on p qubits, such that the pdfs derived above can be directly applied to systems of qubits. Labelling the optical modes as qubit basis states $\{|0\ldots00\rangle,\ |0\ldots01\rangle,\ |0\ldots10\rangle,\ldots,\ |1\ldots11\rangle\}$ we map the optical beamsplitters and phase shifters to single qubit Hadamard gates, and n-qubit logic gates where the state of a single target qubit is transformed depending on the states of $n\ -\ 1$ control qubits. The target qubit operations are the NOT gate or qubit-flip operator, σ_x, and the qubit-phase gates, $\Phi = \mathrm{e}^{\mathrm{i}\phi\sigma_z}$ and $\overline{\Phi} = \sigma_x\Phi\sigma_x$. Each optical phase is mapped to a n-qubit Φ or $\overline{\Phi}$ logic gate, and each optical beamsplitter is mapped as an MZI to a n-qubit Φ or $\overline{\Phi}$ logic gate between two single qubit Hadamard gates on the respective target qubit.

The mapping can be understood with reference to figure 5, which explicitly details the case for 3 qubits and 8 optical modes and present a full circuit example for 2 qubits and 4 optical modes. The target for the n-qubit phase operations is always the final qubit; the conditioning configuration of the control qubits determines which element in the qubit space receives the phase. The addition of Hadamard operations on the final qubit allows the mapping of $1/2$ reflectivity beamsplitters, and therefore MZIs, that operate between pairs of optical modes that differ in labelling only by the final bit. The further addition of n-qubit NOT gates allows MZIs to be mapped from pairs of optical modes that may differ in labelling by more than one bit. Any subset of the MZI operations may be implemented on qubits by simply omitting controlled phases where appropriate.

While not designed to be optimal, this one-to-one mapping between n-qubit phase gates and optical MZIs illustrates one way in which the distributions expressed in figure 2(c) may be used to directly implement a HRU on qubits.

We have presented a recipe to directly generate HRUs in linear optics with a proof that is straightforward in comparison to previous works [6, 23]. Experimental conformation of these results can make use of tomography that does not require further optical circuitry [30]. The formula in its general form is applicable to boson sampling where Haar unitaries are required, and the extension to systems of qubits invites wider applications.

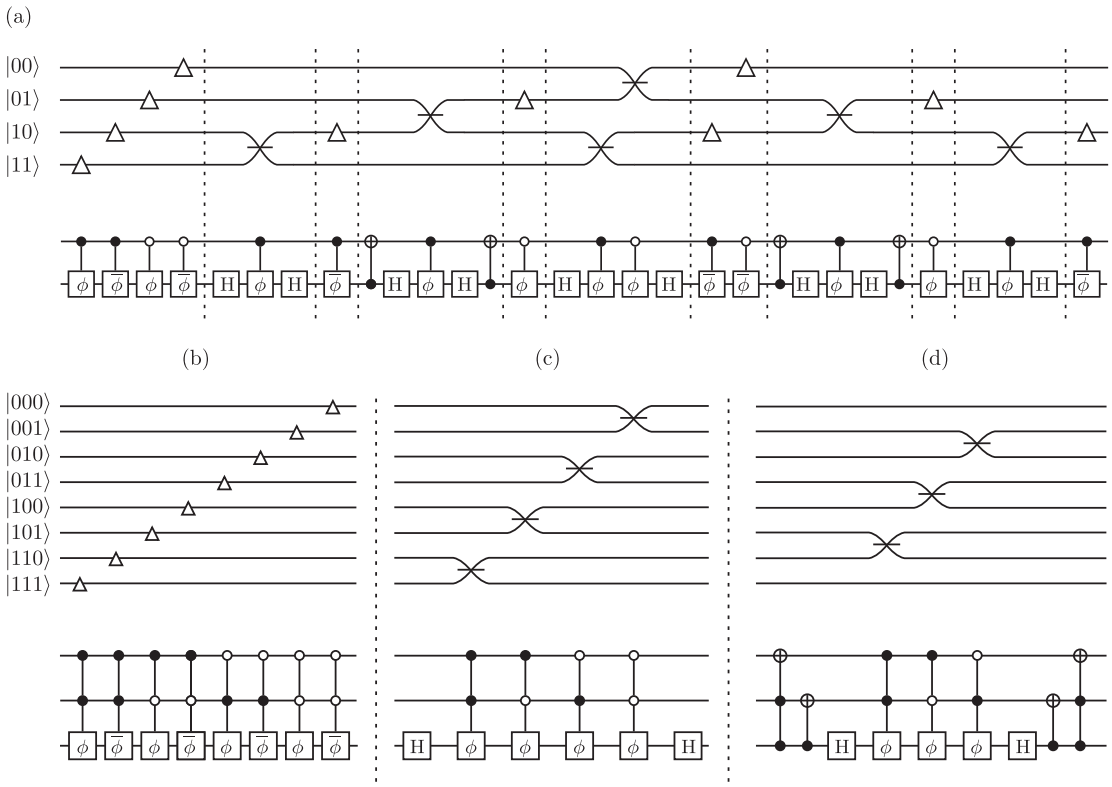

Figure 5. Mapping a linear optical circuit to a unitary on qubits. An empty or solid circle indicates that the operation is conditional on the '0' or '1' state of the control qubit, respectively. (a) A 2-qubit and 4 optical mode example. (b)–(d) the elementary operations for a 3 qubit (8 optical mode) unitary. (b) Phase shifts on single elements in the qubit space result from a judicious choice of conditions for the control qubits. (c) The addition of Hadamard gates allows beamsplitter operations to be implemented on elements in the qubit space that differ only in the state of the final qubit. (d) The further addition of n-qubit-NOT gates allows the mapping of beamsplitters for elements that may differ in the state of more than one qubit.

Acknowledgments

This work was supported by EPSRC, ERC, PICQUE, QUCHIP and the US Army Research Office (ARO), Grant No. W911NF-14-1-0133. JLO'B acknowledges a Royal Society Wolfson Merit Award and a Royal Academy of Engineering Chair in Emerging Technologies. AL and JLO'B acknowledge fellowship support from the Engineering and Physical Sciences Research Council (EPSRC, UK). No data were created during this study.

Appendix. Converting a lower Hessenberg matrix to a lower triangular matrix

We set $J^k_{k-1,0} = 0$ with column operations by subtracting column $\mathbf{c}_k$ multiplied by an appropriate scalar:

$$\mathbf{c}_0^{(k)} = \mathbf{c}_0^{(k-1)} - \mathbf{c}_k \frac{J^{(k-1)}_{k-1,0}}{J_{k-1,k}}. \tag{A.1}$$

The effect on all the other elements of $\mathbf{c}_0$ is to remove the dependence on r_k, which we can prove inductively.

Suppose that after k such operations, the upper k elements of $\mathbf{c}_0$ have been set to zero and the remaining elements have no dependence on r_l for $0 \leqslant l \leqslant k$. We can express the elements of $\mathbf{c}_0^{(k)}$ as:

$$J^{(k)}_{i,0} = \begin{cases} r_{i+1} \prod_{l=k+1}^{i} (1 - r_l), & i \geqslant k, \\ 0, & i < k. \end{cases} \tag{A.2}$$

The base case is $k = 0$, where the expression in (14) corresponds to this general form. We now perform the $(k+1)$th operation on all non-zero rows (i.e. $i \geqslant k+1$):

$$
\begin{aligned}
J_{i,0}^{(k+1)} &= J_{i,0}^{(k)} - \frac{J_{k,0}^{(k)}}{J_{k,k+1}} J_{i,k+1} \\
&= r_{i+1} \prod_{l=k+1}^{i} (1 - r_l) \\
&\quad + \frac{r_{k+1} \prod_{l=k+1}^{k} (1 - r_l)}{r_0 \prod_{l=1}^{k} (1 - r_l)} \frac{r_0 r_{i+1}}{(1 - r_{k+1})} \prod_{l=1}^{i} (1 - r_l) \\
&= r_{i+1} \prod_{l=k+1}^{i} (1 - r_l) + \frac{r_{k+1} r_{i+1}}{(1 - r_{k+1})} \prod_{l=k+1}^{i} (1 - r_l) \\
&= r_{i+1}(1 - r_{k+1}) \prod_{l=k+2}^{i} (1 - r_l) \\
&\quad + r_{i+1} r_{k+1} \prod_{l=k+2}^{i} (1 - r_l) \\
&= r_{i+1}(1 - r_{k+1} + r_{k+1}) \prod_{l=k+2}^{i} (1 - r_l) \\
&= r_{i+1} \prod_{l=k+2}^{i} (1 - r_l).
\end{aligned}
$$

We recover the expression in (A.2), thus proving the result. After $n - 1$ iterations, we find that $J_{n-1,0}^{n-1} = r_n = 1$, recalling that $r_n = 1$ was a variable introduced for convenience.

References

[1] Aaronson S and Arkhipov A 2011 *Proc. 43rd Annual ACM Symp. on Theory of Computing STOC'11* pp 333–42
[2] Crespi A, Osellame R, Ramponi R, Brod D J, Galvao E F, Spagnolo N, Vitelli C, Maiorino E, Mataloni P and Sciarrino F 2013 *Nat. Photon.* **7** 545
[3] Broome M A, Fedrizzi A, Rahimi-Keshari S, Dove J, Aaronson S, Ralph T C and White A G 2013 *Science* **339** 794
[4] Spring J B *et al* 2013 *Science* **339** 798
[5] Tillmann M, Dakic B, Heilmann R, Nolte S, Szameit A and Walther P 2013 *Nat. Photon.* **7** 540
[6] Zyczkowski K and Kuś M 1994 *J. Phys. A: Math. Gen.* **27** 4235
[7] Politi A, Cryan M J, Rarity J G, Yu S and O'Brien J L 2008 *Science* **320** 646
[8] O'Brien J L, Furusawa A and Vučković J 2009 *Nat. Photon.* **3** 687
[9] Marshall G D, Politi A, Matthews J C F, Dekker P, Ams M, Withford M J and O'Brien J L 2009 *Opt. Exp.* **17** 12546
[10] Crespi A, Ramponi R, Osellame R, Sansoni L, Bongioanni I, Sciarrino F, Vallone G and Mataloni P 2011 *Nat. Commun.* **2** 566
[11] Matthews J C F, Politi A, Stefanov A and O'Brien J L 2009 *Nat. Photon.* **3** 346
[12] Smith B J, Kundys D, Thomas-Peter N, Smith P G R and Walmsley I A 2009 *Opt. Exp.* **17** 13516
[13] Laing A, Peruzzo A, Politi A, Verde M R, Hadler M, Ralph T C, Thompson M G and O'Brien J L 2010 *App. Phys. Lett.* **97** 211109
[14] Peruzzo A *et al* 2010 *Science* **329** 1500
[15] Sansoni L, Sciarrino F, Vallone G, Mataloni P, Crespi A, Ramponi R and Osellame R 2012 *Phys. Rev. Lett.* **108** 010502
[16] Carolan J *et al* 2015 *Science* **349** 711
[17] Hayden P, Leung D, Shor P W and Winter A 2004 *Commun. Math. Phys.* **250** 371
[18] Bennett C H, Hayden P, Leung D W, Shor P W and Winter A 2005 *IEEE Trans. Inf. Theory* **51** 56
[19] Abeyesinghe A, Devetak I, Hayden P and Winter A 2009 *Proc. R. Soc.* A **465** 2537
[20] Pranab S 2006 *Proc. 21st Annual IEEE Conf. on Computational Complexity CCC'06* pp 274–87
[21] Reck M, Zeilinger A, Bernstein H J and Bertani P 1994 *Phys. Rev. Lett.* **73** 58
[22] Clements W R, Humphreys P, Metcalf B J, Kolthammer W S and Walmsley I A 2016 *Optica* **3** 1460
[23] Spengler C, Huber M and Hiesmayr B C 2012 *J. Math. Phys.* **53** 013501
[24] Nakata Y, Hirche C, Koashi M and Winter A 2016 Efficient unitary designs with nearly time-independent hamiltonian dynamics arXiv:1609.07021 [quant-ph]
[25] Brandao F G S L, Harrow A W and Horodecki M 2012 Local random quantum circuits are approximate polynomial-designs arXiv:1208.0692
[26] Réffy J 2005 Asymptotics of random unitaries *PhD Thesis* BUTE Institute of Mathematics
[27] Miller D A B 2015 *Optica* **2** 747
[28] Wilkes C M, Qiang X, Wang R, Santagati J, Paesani S, Zhou X, Miller D A B, Marshall G D, Thompson M G and O'Brien J L 2016 60 dB high-extinction auto-configured Mach–Zehnder interferometer (https://doi.org/10.1364/OL.41.005318)
[29] Schaeff C, Polster R, Huber M, Ramelow S and Zeilinger A 2015 *Optica* **2** 523
[30] Laing A and O'Brien J L 2012 Super-stable tomography of any linear optical device arXiv:1208.2868